Consultation on revised Guidance on Consent to Charge – Platform Security Section

Confidential start

[redacted]

Confidential end

Overview of response

The first issue that needs to be identified with this consultation is that it appears to be addressing two separate issues, which should have been dealt with in two separate consultations. There is the issue of robust forms of, and evidence of consent to charge and ensuring that this is obtained correctly, but then the issue of overall platform security is separate to this. We therefore believe that questions 1 to 2 should have been dealt with by a separate consultation and we will be providing our response to this consultation in two separate documents to reflect this.

As detailed in our separate response, we have separated out the issues of Consent to Charge and then Platform Security. This document deals solely with the issue of Platform Security, which we feel should have been dealt with under separate consultation and guidance.

The addition to the current guidance in relation to the Platform Security element is extremely over prescriptive and does not reflect the PSA's own mission of 'applying and enforcing an outcome-based Code of Practice' and 'delivering a balanced approach to regulation'. They are extremely prescriptive and go into far too much detail about what is required of a firm.

Outcomes-based regulation is meant to be used to provide a high level broad outcome, which is to be achieved. The revised guidance does not provide a broad outcome, but detailed prescriptive rules for firms to follow, including what staff must be employed.

There is a continuing theme with our other response, that the general feel of the guidance is extremely over prescriptive but also covers things that should not be included in a guidance note headed Consent to Charge. The Risk issues should be placed under the existing guidance note that follows this topic. The more Guidance Notes the PSA issues, the harder it is for firms to comply as there are so many criteria to comply with from different places. It would be so much easier if each topic was restricted to one guidance note which was updated as and when required. This would also stop PSA guidance notes contradicting each other and firms to be more confused on which part to follow and which part to ignore at times.

We would also like to the raise the issue of the purpose of this consultation. The consultation makes it very clear that the proposed testing should be conducted by firms by the end of the calendar year, with any necessary actions being completed by the end of the 2019/20 financial year. The deadline for responding to the consultation is the 11th October. This clearly shows a lack of consideration by the PSA to consider the responses collected and make amendments to the revised guidance as a result of the feedback. It clearly shows that the PSA intend to implement the revised guidance immediately without consideration to the industry's comments and opinions. Its own Code of Conduct requires reasonable notice to be given for the guidance to be amended, and we do not feel that this constitutes reasonable notice given the impact of the guidance should be completed within 55 working days of the consultation closing.

With regards to the testing conducted, there a number of keys issues with this.

Firstly, that the testing was only conducted on platforms accredited by the MNO's 'Payforit' scheme. If you are going to apply the revised guidance to the whole industry, across all platforms, then surely it needs to be tested on all of the various platforms available to companies and consumers throughout the industry.

Secondly, that the PSA seem unwilling to publish the actual results of the testing, even if anonymised. How can an industry be expected to get behind the revised guidance when they are unaware of the issues it is trying solve? When reviewing the revised guidance, it would be helpful to understand what it is that has caused for such a prescriptive guidance note to be issued. We think this would go some way to appeasing people with the guidance rather than them feeling that the regulator is just being over prescriptive with their regulation. Also, the research was funded by the PSA and MNO's jointly. As the PSA is stakeholder funded, surely the stakeholders are entitled to see the results of the testing that they have funded? The overall feeling of this section of the guidance is that small firms are not welcome in the industry. It is forcing high overheads which the small start-up firms cannot afford, and goes to show that the PSA are not trying to adhere to their own mission statement of 'furthering consumers' interests through encouraging competition, innovation and growth'

Consultation Questions

Q3. Do you agree with the proposed Technical Expectations? If not, why not?

The technical specifications provided seem to only apply when there is a web based interaction with the consumer. As the PSA have refused to release the results of the testing, and only tested on the Payforit platform we can only presume that the current process by keyword opt in is sufficient and that these expectations would not apply to these services.

As we are a firm who does not currently have any services on the Payforit platform or use any web based consent to charge platforms we cannot comment heavily on these expectations.

As there is heavy debate and rumour within the industry of Payforit being removed then rules for platform security on this platform could become obsolete before being implemented.

Q4. Do you agree with the proposed Staffing and Training Expectations? If not, why not?

No. The cost to firms to implement the staffing required under the new guidance is significant, and would put a lot of the providers in the industry out of business. Using the mid-range of the desk research figures in the consultation every platform provider would be looking to up their overheads by £134,000 plus the additional costs of employment to the firm such as NI (approx. £18k), pension (approx. £6k) etc, which has not been taken into consideration.

Other UK regulators do set out the responsibilities that staff must undertake, for example authorised persons with FCA firms, COLP and COFA within SRA regulated firms. These people must undergo a fit and proper persons test to ensure that they are of good character and have the appropriate skills and competence to undertake the role. They take responsibility for the compliance of the firm as a whole with the Code they work under and are accountable for any non-compliance under this role. There is no specification as to the qualifications of this person, merely that they are appropriately experienced to undertake the role. They do not specify the specifics of employees or the roles they must cover as the PSA have included in the guidance. This seems to have gone too far and is certainly not Outcomes-Based regulation.

The other issue that the revised guidance raises, is that of allowing providers to make decisions about other people's businesses. The consultation mentions them being able to have a veto over updates and alterations with the guidance stating that the security team must review and consent to new protocols. It will not always be the case that the Level 1 provider is party to all of the information surrounding a decision due to either confidential or sensitive business material. How can you allow for someone else to make a decision about your company which could stop your business functioning correctly?

Q5. Do you agree with the proposed 'Rick Control' and 'Incident Response' expectations? If not, why not?

Again we feel that this guidance is slightly over prescriptive and already covered in an existing guidance note, Due Diligence; risk assessment, and control on clients. This Guidance details the steps firms should take to ensure that everyone in their value-chain complies with the PSA Code of Conduct, and any extra requirements on firms with regard should be included in this guidance note and not in a separate one. It is making the guidance harder to follow when the PSA splits the guidance on the same topic through different guidance notes. It is difficult to ensure compliance with all the different elements when PSA guidance contradicts itself between different notes.

The guidance includes the requirement for L1's to be able to terminate a payment facility if they think that there has non-compliant activity. Given the number of Level 1 providers within the industry it is entirely possible that L2's use different providers for different portions of their business and for no other reason than it being commercially beneficial. We are aware of L2 providers who use alternative providers to send out their bulk messages. Are you saying that L1 providers who are not necessarily party to the whole picture would be able to stop a payment facility if they did not have evidence of informed consent? What if this was obtained through another provider?

There seems to be a requirement for platform providers to share their platform test results with the MNO's and PSA but the PSA refuse to issue the results of their testing. This could contain commercially sensitive information, and again in our opinion appears to be an apparent attempt for the PSA to obtain more information with regards to the firms it authorises. Surely, a pass or fail would be all that is required of the test provider to give the PSA and MNO's to show that they are compliant with the relevant legislation and regulation? This also does not take into consideration the platform providers which are used who are not regulated by the PSA. They are under no obligation to comply with the Code or Guidance and would therefore not be required to undertake the annual testing. We are therefore assuming that the PSA would take the stance that these merchants would be in breach of the code and guidance, and would be forced to use a PSA platform provider. This is unfair to those who provide services to the industry, but are not themselves required to be regulated, and would also have a financial impact on firms. They have sought contracts with providers for commercial reasons and forcing them to use a PSA regulated firm could increase costs further.